PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04K 1/10, H04L 9/00 — A1

(11) International Publication Number: WO 97/29567

(43) International Publication Date: 14 August 1997 (14.08.97)

(21) International Application Number: PCT/IL97/00044

(22) International Filing Date: 4 February 1997 (04.02.97)

(30) Priority Data:
117085 8 February 1996 (08.02.96) IL

(71) Applicant (*for all designated States except US*): FORTRESS U & T LTD. [IL/IL]; 15 Yehoshua Hatzoref Street, 84106 Beer Sheva (IL).

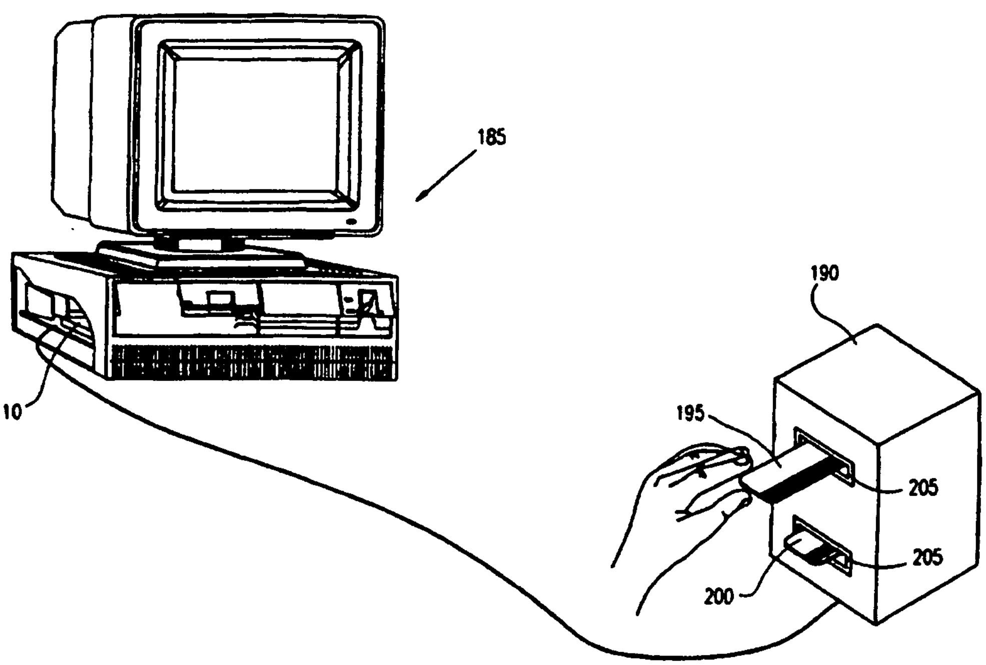
(72) Inventors; and
(75) Inventors/Applicants (*for US only*): GRESSEL, Carmi [IL/IL]; Kvutzat Urim, Mobile Post, 85530 Negev (IL). GRANOT, Ran [IL/IL]; 83 Hasharon Street, 81400 Yavne (IL).

(74) Agents: COLB, Sanford, T. et al.; Sanford T. Colb & Co., P.O. Box 2273, 76122 Rehovot (IL).

(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURE COMPUTER SYSTEM



(57) Abstract

This invention discloses a secure computer including a host CPU (185), and an authenticator computer (190), wherein both the host CPU and the authenticator computer are embedded in a single package.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgystan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic			SE	Sweden
CG	Congo	KR	Republic of Korea	SG	Singapore
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LR	Liberia	SZ	Swaziland
CS	Czechoslovakia	LT	Lithuania	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	LV	Latvia	TJ	Tajikistan
DK	Denmark	MC	Monaco	TT	Trinidad and Tobago
EE	Estonia	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	UG	Uganda
FI	Finland	ML	Mali	US	United States of America
FR	France	MN	Mongolia	UZ	Uzbekistan
GA	Gabon	MR	Mauritania	VN	Viet Nam

SECURE COMPUTER SYSTEM

FIELD OF THE INVENTION

The present invention relates to secure computer systems in general.

BACKGROUND OF THE INVENTION

The need for secure computer systems is well known. The need for secure computer systems falls into several categories. The need for secure capabilities which enable a computer to work in a secure environment, such as an electronic mail, remote banking, Internet, secure communications, telefax, or smart card environment is well known and falls into a first category of need. In a second category of need, it is well known that expensive computer CPU chips are often subject to theft. Unfortunately, individual expensive CPU chips can not easily be identified, and hence the recovery of stolen CPU chips is difficult. There is therefore a need to protect expensive CPU chips.

Methods and apparatus useful in secure computing are described in the following patent applications, commonly owned with the present application, the disclosures of which are hereby incorporated herein by reference:

Israel patent applications 113375 and 115534; and

United States patent applications 08/154,220 and 08/437,223.

Methods and apparatus useful in secure computing are described in the following publications:

D. E. Denning and M. Smid, "Key escrowing today", IEEE Communication Magazine, September 1994, pp. 58 - 68;

C. Gressel, R. Granot, and I. Dror, "International Cryptographic Communication Without Key Escrow", International Cryptographic Institute '95, Washington DC, September 22, 1995;

R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM Vol. 21 #2, February 1978, pp. 120-126;

DES Modes of Operation, FIPS PUB 81, National Bureau of Standards, US Department of Commerce, Washington, DC, 1981;

MC68HC05SC49, 8-bit microcomputer with EEPROM and N modulo M exponent coprocessor product preview, Motorola semiconductor technical data, Schaumburg IL, 1993;

MC68HC05SC30, Enhanced 8-bit microcomputer with EEPROM and N modulo M exponent coprocessor product preview, Motorola semiconductor technical data, Schaumburg, IL 1993;

ST16xF74 CMOS crypto-computer family ST16xF74, SGS-Thomson Microelectronics, Agrate, Italy, October 1993;

ST16CF54 CMOS MCU based safeguarded smartcard IC with modular arithmetic processor, SGS-Thomson Microelectronics, Agrate, Italy, September 1994; and

Cryptoprocessor chip includes embedded cryptolibrary, SGS-Thomson Microelectronics, Agrate, Italy, press release K491M, October 1994.

The disclosures of the above publications and of the publications cited therein are hereby incorporated by reference. The disclosures of all publications mentioned in this specification and of the publications cited therein are hereby incorporated by reference.

SUMMARY OF THE INVENTION

The present invention seeks to provide an improved secure computer system. In the present invention, an authenticator computer is embedded in the same package with a host CPU. The embedded authenticator computer may provide secure capabilities such as those described above. The embedded authenticator computer may also provide identifying information including proof of identity. The identifying information may aid in preventing theft of the computer system and/or may aid in identification of a stolen computer system. Because the authenticator computer is embedded in the same package with the host CPU, removing the authenticator computer in order to circumvent the anti-theft capabilities thereof will generally be very difficult and/or too expensive to attempt.

There is thus provided in accordance with a preferred embodiment of the present invention a secure computer including a host CPU and an authenticator computer, wherein both the host CPU and the authenticator computer are embedded in a single package. The authenticator computer may have an identity and, and the authenticator computer may provide proof of the identity upon receiving an external signal from a verifying device. The proof of the identity may include origin information and/or an audit trail.

The secure computer may also include a smart card receiver, which may comprise a reader/writer card, including at least one smart card acceptor socket, each smart card acceptor acceptor socket being adapted to receive a smart card, wherein the authenticator verifies the smart card. The at least one smart card acceptor socket may include a plurality of smart card acceptor sockets.

The authenticator may control access to a controlled device. The authenticator provides data protection, including data encryption and/or data decryption. The data protection may include providing and/or verifying a digital signature.

The authenticator may protect data transmission between the secure computer and a remote device, optionally using approved protocols for transnational encryption, as well as approved protocols for authentication origin and contents of documents using an electronic signature.

There is also provided in accordance with another preferred embodiment of the present invention a method for securing a host computer, the method including providing a host CPU, providing an authenticator computer, and embedding both the host CPU and the authenticator computer in a single package.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a simplified pictorial illustration of a secure computer system constructed and operative in accordance with a preferred embodiment of the present invention;

Figs. 2A - 2C are simplified pictorial illustrations of alternative preferred embodiments of the system of Fig. 1, comprising alternative embodiments thereof for different packaging methods;

Fig. 3 is a simplified flowchart illustration of a preferred method of operation of the secure computer system 10 of Fig. 1;

Fig. 4 is a simplified pictorial illustration of an alternative preferred embodiment of the present invention;

Fig. 5 is a simplified pictorial illustration of a further alternative preferred embodiment of the present invention;

Fig. 6 is a simplified pictorial illustration of a still further alternative preferred embodiment of the present invention; and

Fig. 7 is a simplified block diagram illustration of the secure computer system of Fig. 1.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Fig. 1 which is a simplified pictorial illustration of a secure computer system 10 constructed and operative in accordance with a preferred embodiment of the present invention. The secure computer system 10 comprises an authenticator computer 20. The authenticator computer 20 may be any appropriate authenticator computer, such as a cryptocomputer chip or a computer chip designed to rapidly process modular arithmetic operations useful for performing authentication, encryption, and decryption, as is well known in the art. Preferably, the authenticator computer 20 may be a model ST16CF54 available from SGS-Thomson. The authenticator computer 20 may alternatively be a MC68HC05SC49 8-bit microcomputer, commercially available from Motorola, Schaumburg IL, USA.

The authenticator computer 20 is embedded in a single package with a host CPU 30. The host CPU 30 may be any appropriate CPU. It is appreciated that the present invention, by providing anti-theft capabilities, is particularly useful in the case where the host CPU 30 is an expensive CPU.

Preferably, in order to provide optimal anti-theft capabilities, the embedding of the authenticator computer 20 and the host CPU 30 into a single package comprises permanently bonding together the authenticator computer 20 and the host CPU 30. The system of Fig. 1 also comprises an electrically insulating thermally conducting layer 32, covering the authenticator computer 20 and the host CPU 30. The electrically insulating thermally conducting layer 32 may comprise ceramic or any other suitable electrically insulating thermally conducting material. It is appreciated that alternative and/or additional methods of bonding the authenticator computer 20 and the host CPU 30 may be used, such as, for example, providing a bonding layer (not shown) between the authenticator computer 20 and the host CPU 30.

The system of Fig. 1 also comprises an external connection 35. The external connection 35 shown in Fig. 1 is arranged, by way of example only, into two smart card reader connectors 37. The external connection 35, which typically comprises a plurality of pins, is operative to provide an electrical connection between the authenticator computer and external devices, such as one or more smart card readers. The external connection 35 may also be operative to provide an electrical connection to an external device comprising a verification device, as described below with reference to Fig. 6.

The term "smart card reader", as used throughout the present specification and claims, refers to any smart card device, as is well known in the art, or to any device using similar technology to provide authentication and/or transaction security. It is appreciated that a smart card device may accept a card, a key, a button, or any portable security identification item. The card, key, button, or any portable security identification item is referred to throughout the present specification and claims as a "smart card". Typically, a smart card device, as is well known in the art, comprises an imbedded processor and/or memory unit which are operative to provide the authentication and/or transaction security.

Reference is now additionally made to Figs. 2A - 2C, which are simplified pictorial illustrations of alternative preferred embodiments of the system of Fig. 1, comprising alternative embodiments thereof for different packaging methods. The packaging methods of Figs. 2A - 2C are believed to simplify the interface between the secure computer system 10 and a computer in which the secure computer system 10 is located, particularly by not occupying additional motherboard space or requiring changes to the motherboard.

Fig. 2A is an exploded view of the secure computer system 10 of Fig. 1, packaged using a lead frame packaging method. The system of Fig. 2A also comprises an adaptor 40, which is operative to connect to a plurality of conductors 42 formed on the surface of the host CPU 30. The authenticator computer 20 is in turn operatively connected to the adaptor 40. The host CPU 30 is typically positioned on top of the adaptor 40, with the adaptor 40 being positioned on top of the authenticator computer 20; this arrangement is deemed preferable in order to allow sufficient thermal conductance of the host CPU 30. It is appreciated that other physical arrangements of the authenticator computer 20, the host CPU 30, and the adaptor 40 are also possible. The adaptor 40 is operative to provide an electrical connection between the host CPU 30 and the authenticator computer 20, and also to provide an electrical connection via the external connection 35 to external devices, as explained above.

Fig. 2B is a simplified pictorial illustration of the secure computer system 10 of Fig. 1, packaged using a socketed packaging method. The packaging method of Fig. 2B is believed to be particularly useful when adding the authenticator computer 20 to an existing computer system. The system of Fig. 2B comprises an adaptor 45. The adaptor 45 comprises a plurality of conductor pins 50, designed to fit within an existing acceptor socket adapted to receive the host CPU 30. The adaptor 45 also comprises an external connector 35, as described above.

The adaptor 45 is adapted to receive the authenticator computer 20, typically inside the adaptor 45. The adaptor 45 is also adapted to receive the host computer 30, typically on top of the adaptor 45. The adaptor 45 is operative to provide an electrical connection between the host CPU 30 and the authenticator computer 20, and also to provide an electrical connection via the external connection 35 to external devices, as explained above.

Fig. 2C is an exploded view of the secure computer system 10 of Fig. 1, packaged using a pin grid array packaging method. The system of Fig. 2C comprises a pin grid board 55, comprising a plurality of pins 60. At least some of the plurality of pins 60 extend upward above the pin grid board 55, allowing connection to an authenticator printed circuit board (PC board) 65. The host CPU 30 is mounted to the PC board 65, typically on the upper side thereof, so that a plurality of pins (not shown) on the underside of the host CPU 30 extend through holes in the PC board 65 and make electrical contact with the plurality of pins 60. The authenticator computer 20 is mounted on the pin grid board 55, typically on the upper side thereof. The PC board 65 is operative to provide an electrical connection between the host CPU 30 and the authenticator computer 20, and also to provide an electrical connection via the external connection 35 to external devices, as explained above.

It is appreciated that the embodiments of Figs. 2A - 2C are provided by way of example only, and that a wide variety of packaging methods may be used in packaging the secure computer system 10 of Fig. 1.

The operation of the system of Fig. 1 is now briefly described. The secure computer system 10 may receive a request to be processed from an external device through the external connection 35 and operate thereon. Requests may also be processed internally; that is, a request may be initiated by the host CPU 30 and may then be processed by the authenticator computer 20. In the case of either an external or an internal request, the output of processing the request by the authenticator computer 20 may be provided either through the external connection 35 or to the host CPU 30, which typically further processes the output. Typically, a request comprises a request to perform one of the following: a digital signature operation; a data transmission protection operation; a data protection operation; an access control operation; a smart card verification operation; or and proof of identity operation.

Reference is now made to Fig. 3, which is a simplified flowchart illustration of a preferred method of operation of the secure computer system 10 of Fig. 1. The method of Fig. 3 preferably includes the following steps:

The authenticator computer 20 receives a request, either an internal request from the host CPU 30 or an external request from an external device (step 100). The request is then processed according to the type of request.

If the request is to perform a digital signature operation, that is, to verify or provide a digital signature, as is well known in the art, the authenticator computer 20 performs the digital signature operation (step 110). Digital signature operations are described, for example, in R. L. Rivest, A. Shamir, and L. Adleman, referred to above. Typically, the request to provide a digital signature operation is received from the host CPU 30 and the result of the digital signature operation is output to the host CPU 30 for further processing.

If the request is to protect a data transmission, the authenticator computer 20 protects the data transmission (step 120). Typically, protection of a data transmission may include data encryption, data decryption and data verification, as is well known in the art. Protection of a data transmission may also include using an approved transnational protocol for protecting a data transmission, such as, for example, that described by C. Gressel, R. Granot, and I. Dror, referred to above. Other relevant apparatus and methods are also described in Israel patent applications 113375 and 115534, and in United States patent application 08/437,223. Typically, the data to be protected is received from the host CPU 30 and the result of the data protection operation is output to the host CPU 30 for further processing.

Reference is now additionally made to Fig. 4, which is a simplified pictorial illustration of an alternative preferred embodiment of the present invention. The embodiment of Fig. 4 is especially applicable for use with step 120 of Fig. 3. The system of Fig. 4 comprises a computer 170, the computer 170 comprising the secure computer system 10. The computer 170 is operative to transmit data over a remote data link 175 to a remote computer system 180. Protection of data transmission is provided by the secure computer system 10, as described above.

If the request is to provide data protection, such as, for example, to encrypt or decrypt data which is under control of the host CPU 30, the authenticator computer 20 provides the data protection (step 130). The data protection may comprise encryption or decryption methods which are well known in the art and are described, for example, in DES Modes of Operation, referred to above. Typically, the result of the data protection operation is output to the host CPU 30 for further processing.

If the request is to control access to an external device, the access control request is processed by the authenticator computer 20 (step 140). The external device may comprise any appropriate external device such as, for example, any of the following: a computerized device; a computer peripheral device; a locked door; or any other locked access apparatus. Processing of the access control request typically comprises receiving a request, typically from the host CPU 30 and verifying that the request is legitimate. Verifying that the request is legitimate may be performed using any appropriate method, such as a method well known in the art, for example the methods described in R. L. Rivest, A. Shamir, and L. Adleman, referred to above.

If the request is to verify a smart card, the smart card is verified (step 150). Smart cards, as is well known in the art, may be used in a wide variety of ways, including the following: to store identifying information about an individual; to store personal or medical information about an individual; and/or to store financial information for use in carrying out transactions. Verifying the smart card may include verifying that the smart card is valid, as is well known in the art. Verifying the smart card may also include reading data from the smart card, as is well known in the art. Verifying the smart card may also include carrying out a financial transaction based on information stored in the smart card, as is well known in the art. Methods for verifying a smart card include those described in R. L. Rivest, A. Shamir, and L. Adleman, referred to above.

Reference is now additionally made to Fig. 5, which is a simplified pictorial illustration of a further alternative preferred embodiment of the present invention. The system of Fig. 5 comprises a computer 185, the computer 185 comprising the secure computer system 10. The computer 185 is operatively attached to a smart card receiver 190. The smart card receiver 190 is operative to receive a first smart card 195 and, optionally, a second smart card 200 in one or more smart card acceptor sockets 205. It is appreciated that the smart card acceptor sockets 205 are adapted to accept the particular form of the smart cards 195 and 200 chosen for use, and that the card form is shown in Fig. 5 by way of example only.

When the second smart card 200 is used, the first smart card 195 typically represents customer information in a financial transaction, and the second smart card 200 typically represents merchant information or bank teller information in a financial transaction. The secure computer system 10 is operative to verify the first smart card 195 and, optionally, the second smart card 200, as described above. It is appreciated that by using both the first smart card 195 and the second smart card 200 it is possible to record proof of a transaction

both on the smart card belonging to the customer such as, for example, the first smart card 195 and on the smart card belonging to the bank such as, for example, the second smart card 200. The transaction proof typically comprises digital signatures of both the customer and the bank teller.

Processing of the smart card verification request typically comprises the authenticator computer 20 receiving a request, typically from the host CPU 30, and verifying that the request is legitimate, with output of the verification being sent to the host CPU 30.

If the request is to provide proof of identity, the authenticator computer 20 provides proof of identity (step 160). Typically, proof of identity comprises proof of identity of the host CPU 30. By storing identity information identifying the host CPU 30, the authenticator computer 20 provides an identification function which may aid in preventing or deterring theft of the host CPU 30. Proof of identity may also comprise proof of identity of a user who requests access to certain protected files or data, in which case proof of identity establishes the user's access rights.

Reference is now additionally made to Fig. 6, which is a simplified pictorial illustration of a still further alternative preferred embodiment of the present invention. The system of Fig. 6 comprises the secure computer system 10. The system of Fig. 6 further comprises a verification unit 210, operatively attached to the secure computer system 10. The connection between the verification unit 210 and the secure computer system 10 is preferably a temporary connection which can be easily made and broken, and preferably comprises a connection to a minimum number of pins within the external connection 35 such as, for example, two pins. The connection between the verification unit 210 and the secure computer system 10 is preferably such that the connection may be made and broken whether or not the secure computer system 10 is installed in a computer.

The verification unit 210 is operative to send a signal to the secure computer system 10, preferably comprising an identification of the verification unit 210. The secure computer system 10 receives the signal and preferably verifies the signal, using verification methods well known in the art, to ensure that the verification unit 210 is authorized to request proof of identity. If the verification unit 210 is so authorized, the secure computer system 10 provides the verification system 210 with proof of identity, which may be displayed by the verification unit 210, stored in the verification unit 210, and or output by the verification unit 210.

Proof of identity preferably comprises at least one of the following: serial number; origin, including at least one of manufacturer, date of production, place of production, and batch run of production; and information about a computer or other electronic product or other object in which the secure computer system 10 is used. It may also include public key certificates necessary for controlled use of licensed software. It is appreciated that proof of identity may comprise information relating to one or more of the following: the identity of the secure computer system 10; the identity of the authenticator computer 20; the identity of the host CPU 30; and the identity of the computer of other electronic product or other object in which the secure computer system 10 is used. Proof of identity may also include an audit trail typically comprising historical information concerning the manufacture and use of the secure computer system 10.

Reference is now made to Fig. 7, which is a simplified block diagram illustration of the secure computer system 10 of Fig. 1. The system of Fig. 7 is self-explanatory, except as follows. The external connection 35 is preferably fused, to prevent application of an external over-voltage from damaging the authenticator computer 20 and thus removing the authenticator computer 20 from operation. Such damage might allow access without intervention by the authenticator computer 20 destroying the authenticator with the unique identity allowing the use of a stolen CPU.

It is appreciated that the software components of the present invention may, if desired, be implemented in ROM (read-only memory) form. Preferably, in the present invention a ROM would be electrically programmable and masked on during silicon fabrication. Preferably most of the program would be masked in the fabrication. Keys would be generated internally with the real random number generator and stored electrically programmable ROM and propriety program can be downloaded by a trusted third party using protocols as mentioned above. The software components may, generally, be implemented in hardware, if desired, using any conventional techniques.

It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

It will be appreciated by persons skilled in the art that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention is defined only by the claims that follow:

CLAIMS

1. A secure computer comprising:

a host CPU; and

an authenticator computer,

wherein both the host CPU and the authenticator computer are embedded in a single package.

2. Apparatus according to claim 1 wherein the authenticator computer has an identity and wherein the authenticator computer provides proof of the identity upon receiving an external signal from a verifying device.

3. Apparatus according to claim 2 wherein the proof of the identity comprises origin information.

4. Apparatus according to claim 3 wherein the proof of the identity also comprises an audit trail.

5. Apparatus according to claim 1 and also comprising a smart card receiver comprising at least one smart card acceptor socket, each said smart card acceptor socket being adapted to receive a smart card,

wherein the authenticator verifies the smart card.

6. Apparatus according to claim 5 wherein the at least one smart card acceptor socket comprises a plurality of smart card acceptor sockets.

7. Apparatus according to either claim 5 or claim 6 wherein the authenticator controls access to a controlled device.

8. Apparatus according to claim 1 wherein the authenticator provides data protection.

9. Apparatus according to claim 8 wherein the data protection comprises data encryption.

10. Apparatus according to claim 8 wherein the data protection comprises data decryption.

11. Apparatus according to claim 9 wherein the data protection comprises data decryption.

12. Apparatus according to any of claims 8 - 11 wherein the data protection comprises providing a digital signature.

13. Apparatus according to claim 8 wherein the data protection comprises verifying a digital signature.

14. Apparatus according to claim 9 wherein the data protection comprises verifying a digital signature.

15. Apparatus according to claim 10 wherein the data protection comprises verifying a digital signature.

16. Apparatus according to claim 11 wherein the data protection comprises verifying a digital signature.

17. Apparatus according to claim 12 wherein the data protection comprises verifying a digital signature.

18. Apparatus according to claim 1 wherein the authenticator protects data transmission between the secure computer and a remote device.

19. Apparatus according to claim 18 wherein the authenticator protects data transmission using approved protocols for transnational encryption.

20. A method for securing a host computer, the method comprising:

providing a host CPU;

providing an authenticator computer; and

embedding both the host CPU and the authenticator computer in a single package.

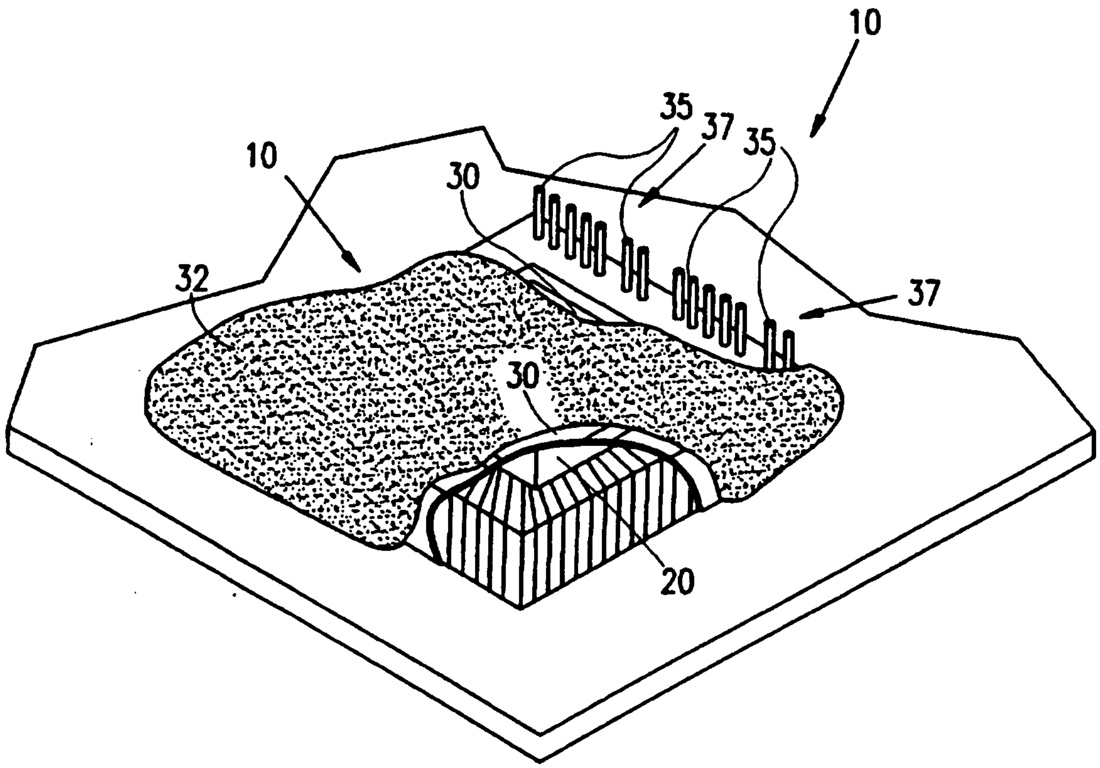


FIG. 1

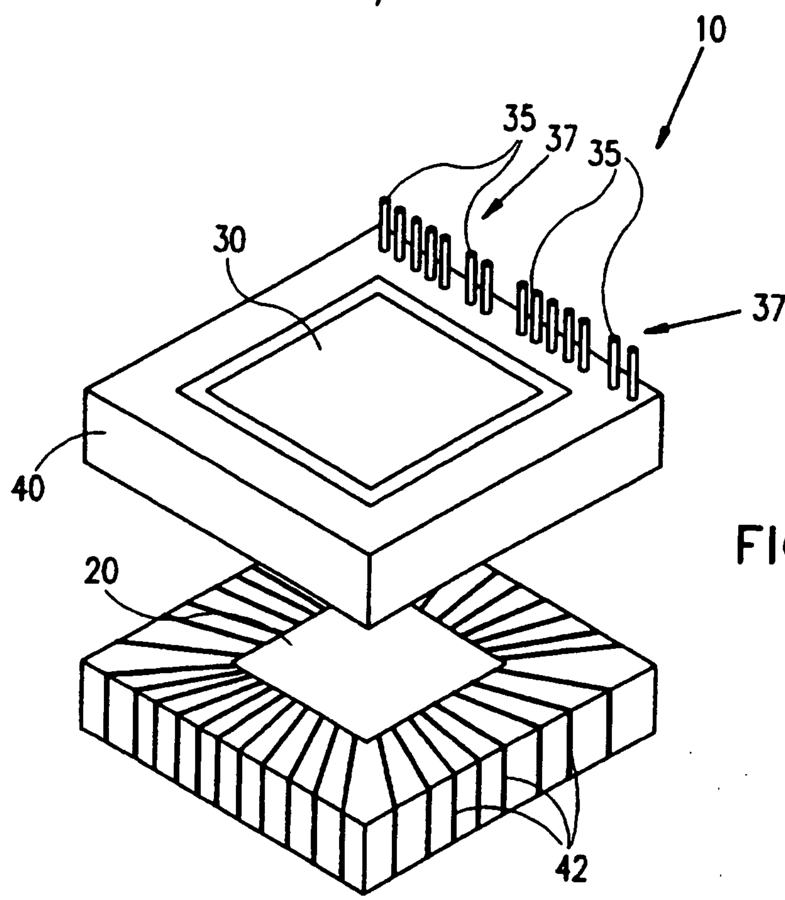


FIG. 2A

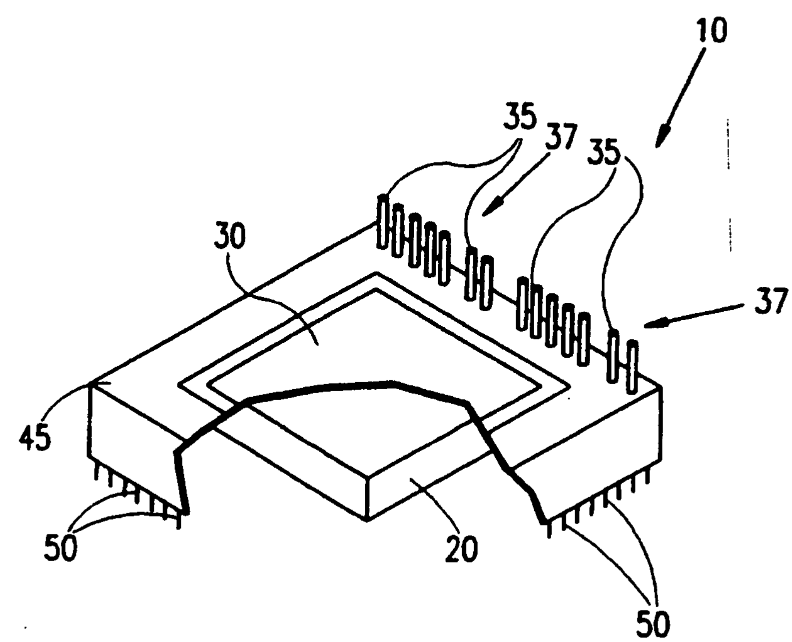


FIG. 2B

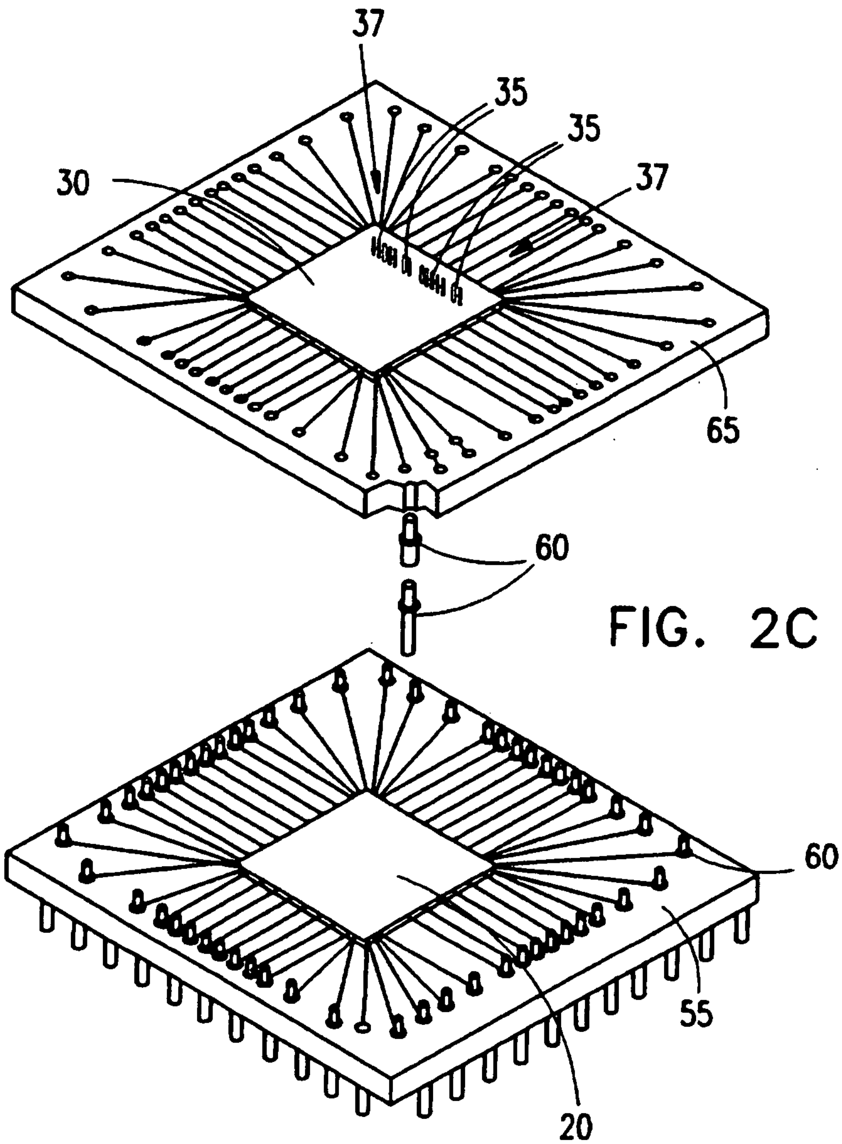
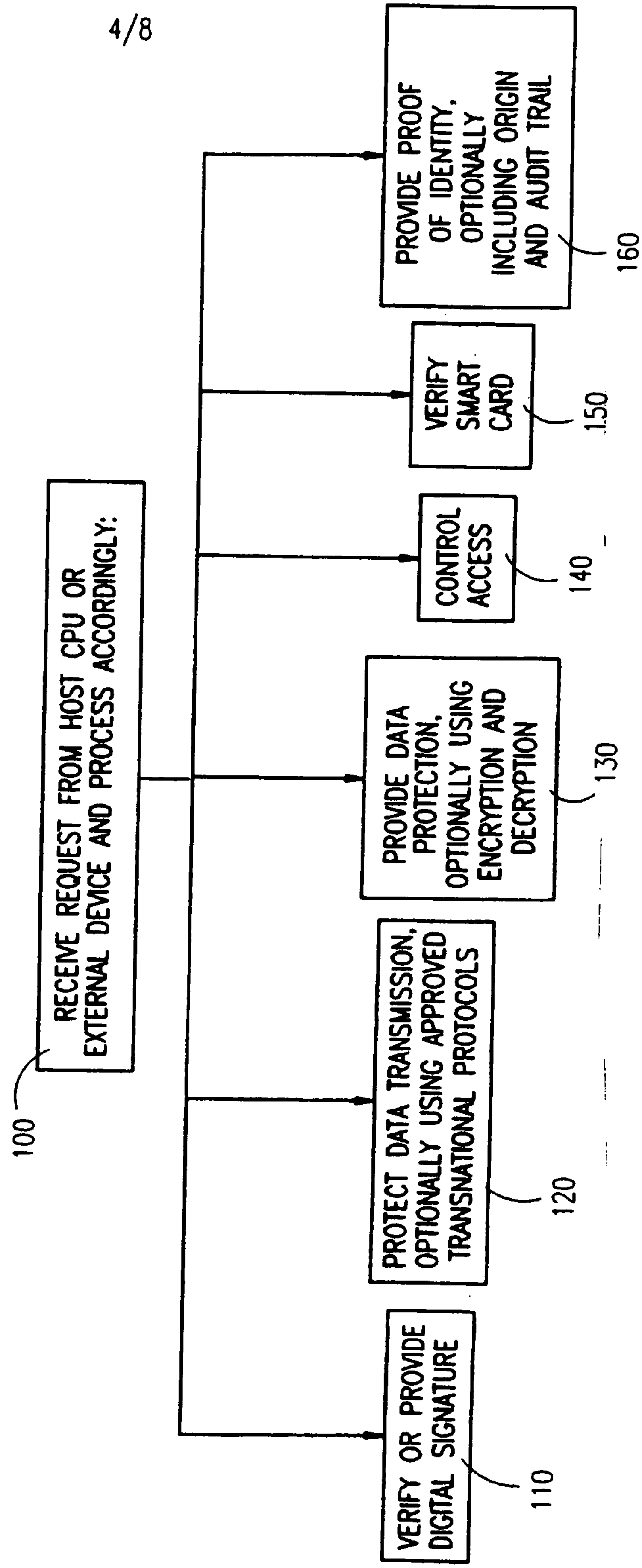


FIG. 2C

FIG. 3


RECEIVE REQUEST FROM HOST CPU OR EXTERNAL DEVICE AND PROCESS ACCORDINGLY:
100
VERIFY OR PROVIDE DIGITAL SIGNATURE
110
PROTECT DATA TRANSMISSION, OPTIONALLY USING APPROVED TRANSNATIONAL PROTOCOLS
120
PROVIDE DATA PROTECTION, OPTIONALLY USING ENCRYPTION AND DECRYPTION
130
CONTROL ACCESS
140
VERIFY SMART CARD
150
PROVIDE PROOF OF IDENTITY, OPTIONALLY INCLUDING ORIGIN AND AUDIT TRAIL
160

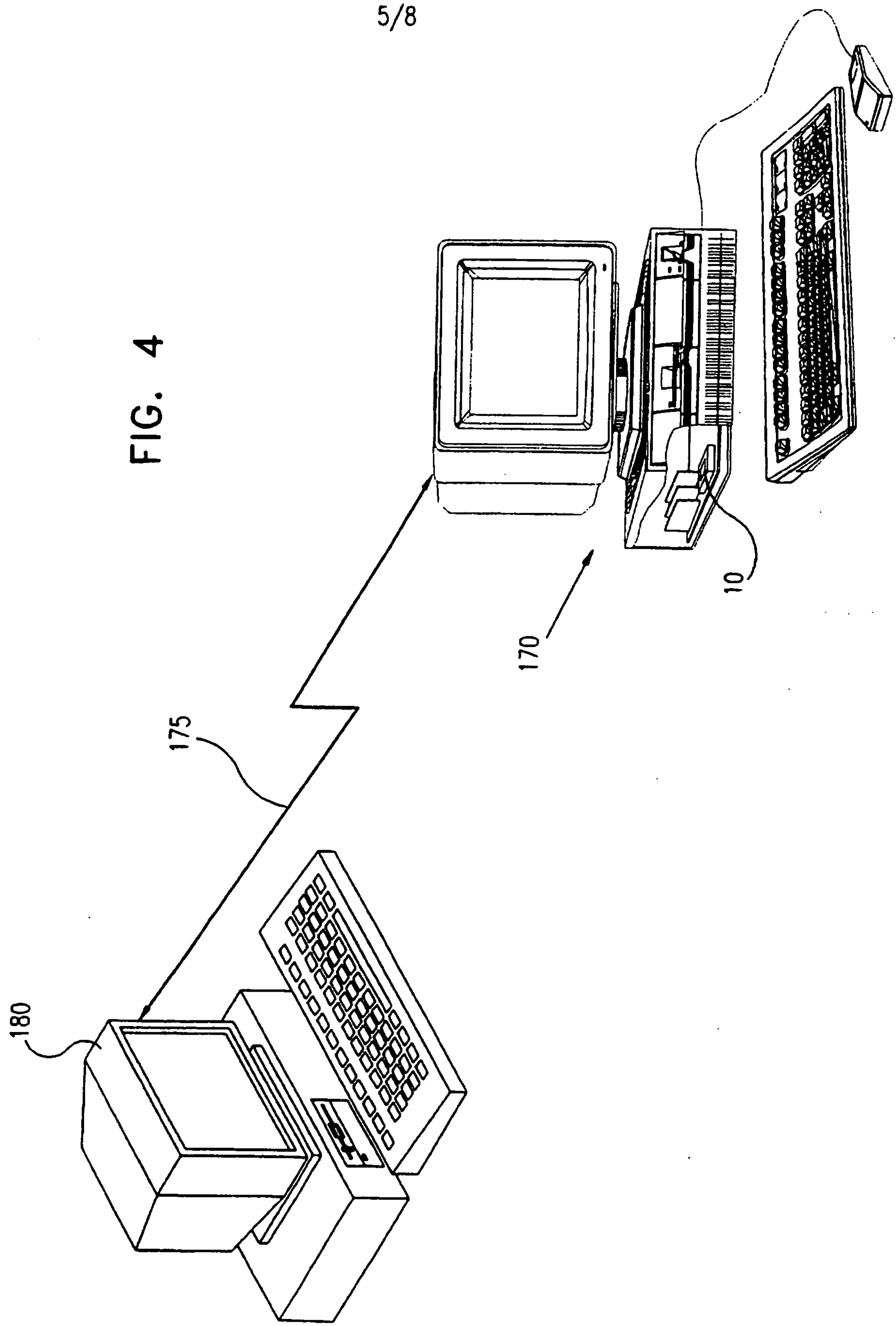


FIG. 4

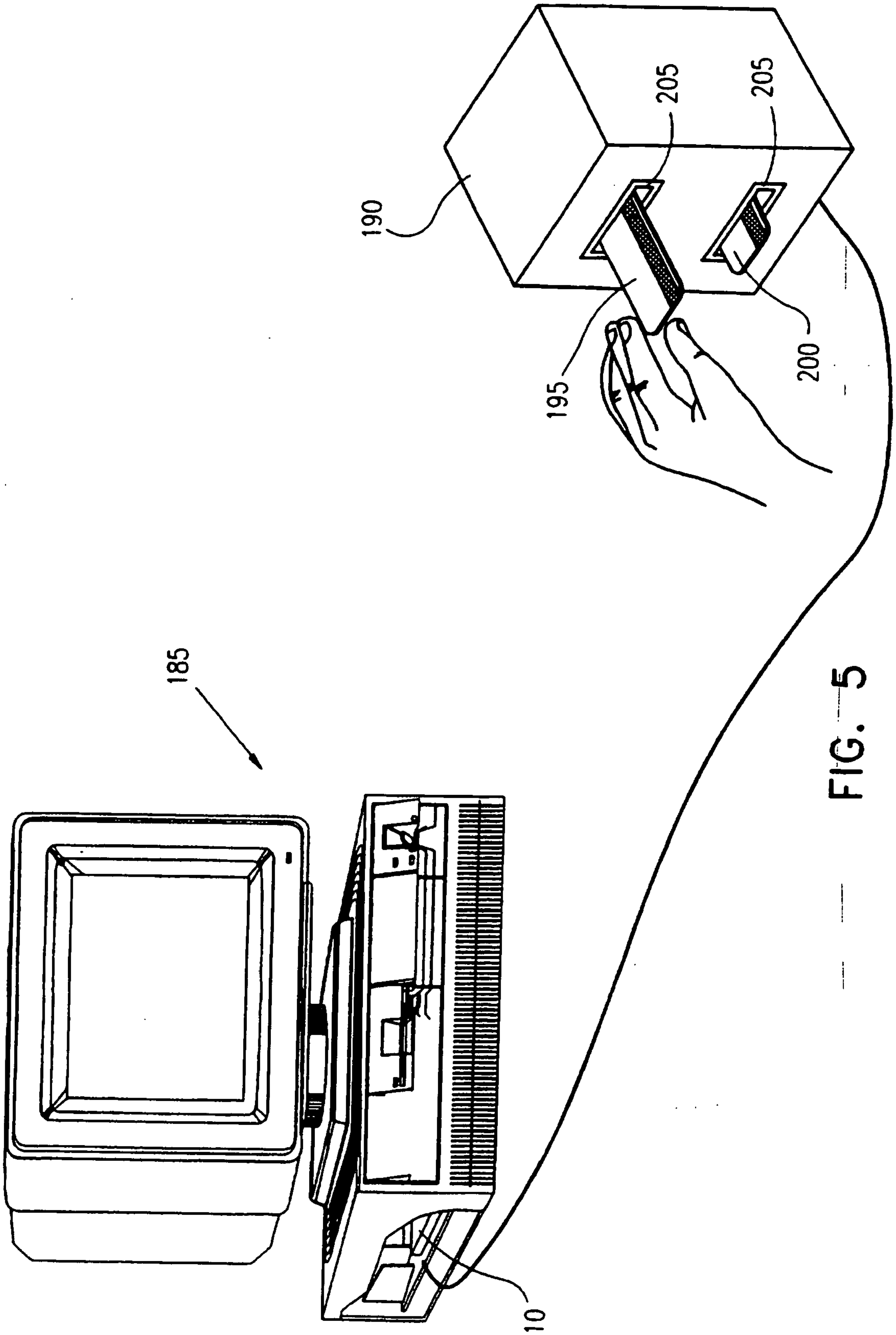


FIG. 5

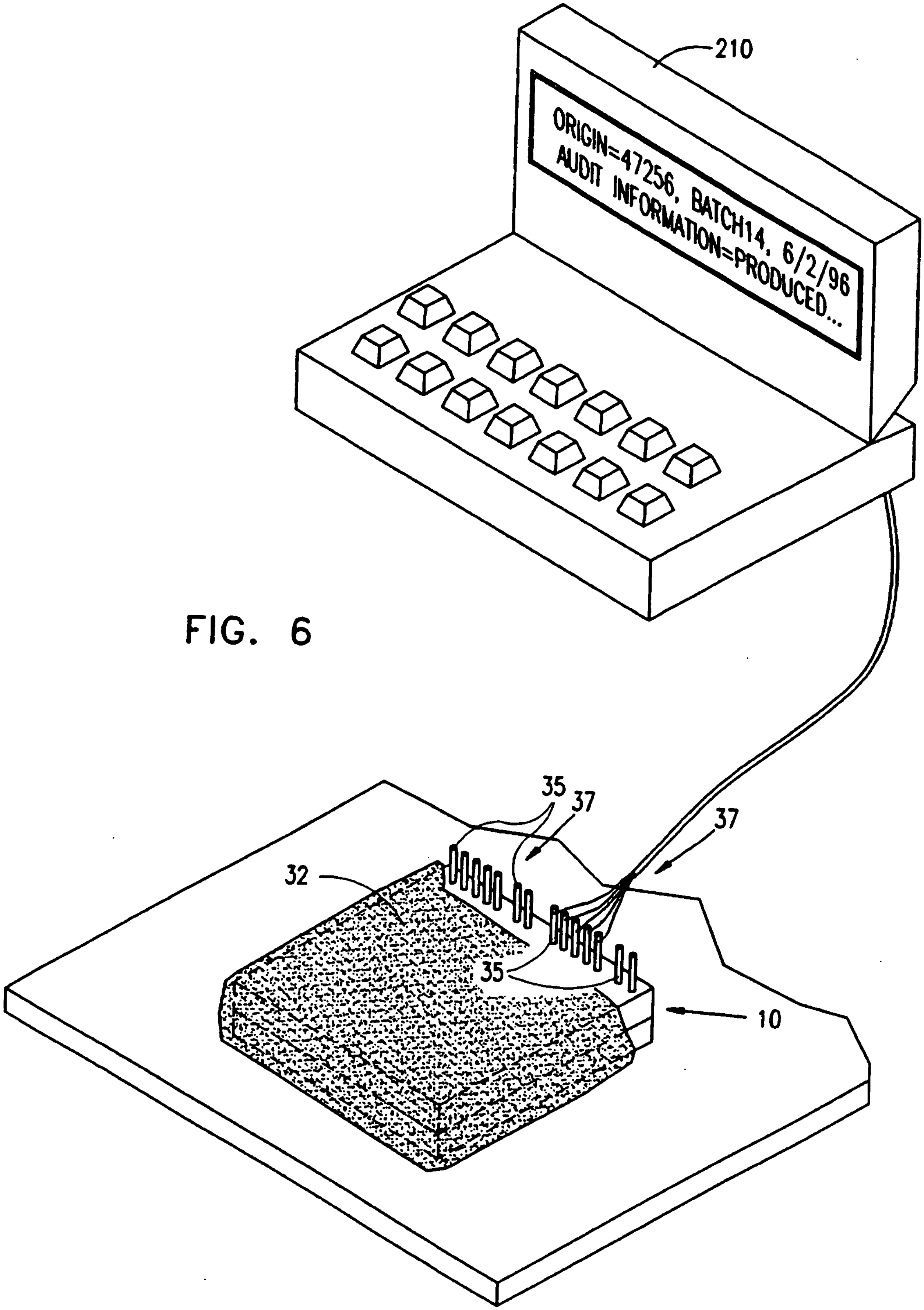
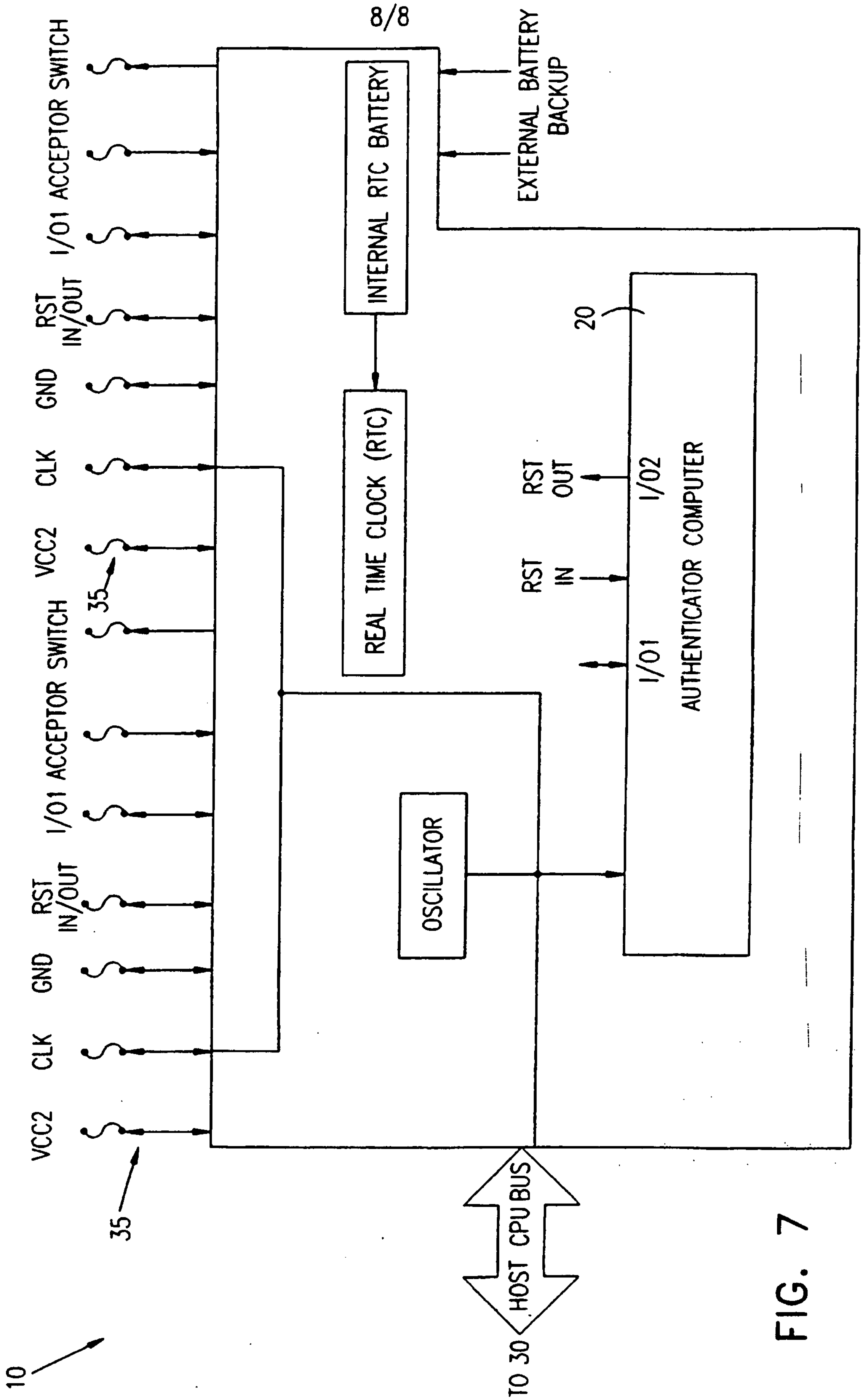

210
ORIGIN=47256, BATCH14, 6/2/96
AUDIT INFORMATION=PRODUCED...
35
37
37
32
35
10

FIG. 6



I/01 ACCEPTOR SWITCH
RST IN/OUT
GND
CLK
VCC2
35
I/01 ACCEPTOR SWITCH
RST IN/OUT
GND
CLK
VCC2
35
INTERNAL RTC BATTERY
REAL TIME CLOCK (RTC)
EXTERNAL BATTERY BACKUP
OSCILLATOR
20
RST OUT
RST IN
I/02
I/01
AUTHENTICATOR COMPUTER
HOST CPU BUS
TO 30
10

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL97/00044

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04K 1/10; H04L 9/00
US CL :380/23; 395/186
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/23, 25; 395/186, 188.01

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, STN (WPIDS)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,200,999 A (MATYAS et al.) 06 April 1993, see the abstract, col. 9, line 56 to col. 10, line 49	1-20
Y	US 5,265,164 A (MATYAS et al.) 23 November 1993, see the abstract, figures 5, 10	1-20
Y,P	US 5,535,276 A (GANESAN) 09 July 1996 , see the abstract; also col. 8, line 9-67	1-20
Y,P	US 5,546,463 A (CAPUTO et al.) 13 August 1996, see the abstract; figure 1C; col. 4, line 24 to col.5, line 15	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

22 APRIL 1997

Date of mailing of the international search report

02 JUN 1997

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
ALBERT DECADY
Telephone No. (703) 308-3900